(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020030088643 A
(43)Date of publication of application: 20.11.2003

(21)Application number: 1020020026463
(22)Date of filing: 14.05.2002
(71)Applicant: SAMSUNG ELECTRONICS CO., LTD.
(72)Inventor: HAN, GYEONG EUN
KIM, A JEONG
KIM, SU HYEONG
KIM, YEONG CHEON
LEE, MIN HYO
NOH, SEON SIK
PARK, HYEOK GYU
SONG, JAE YEON

(51)Int. Cl H04L 9/30

(54) CODING METHOD IN GIGABIT ETHERNET-PASSIVE OPTICAL NETWORK

(57) Abstract:

PURPOSE: A coding method in a gigabit ethernet-passive optical network is provided to improve the efficiency of encryption by including the exchange and manage of an encryption key into a scheduling procedure of the gigabit ethernet-passive optical network.

CONSTITUTION: An optical line terminal(100) of an optical network unit(120) is registered(801,803,805). The optical line terminal(100) of optical network unit(120) is authenticated(807,809,811). The optical line terminal(100) generates a session key using an obtained public key of the optical network unit(120) in the authentication process, and the pseudo-random values. The optical line terminal(100) transmits the pseudo-random values to the optical network unit(120). The optical network unit(120), which receives the pseudo-random values, generates a session key using the received pseudo-random values and the public key of the optical line terminal(100).

Legal Status

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 9/30

(11) 공개번호 특2003-0088643
(43) 공개일자 2003년11월20일

(21) 출원번호 10-2002-0026463
(22) 출원일자 2002년05월14일

(71) 출원인 삼성전자주식회사
대한민국
442-742
경기도 수원시 팔달구 매탄3동 416번지

(72) 발명자 김수형
대한민국
463-020
경기도성남시분당구수내동금호아파트103-1001

송재연
대한민국
156-809
서울특별시동작구대방동376-2218/1

김영천
대한민국
560-250
전라북도전주시완산구중화산동한신코아아파트2동905호

김아정
대한민국
140-731
서울특별시용산구이태원2동청화아파트5동805

노선식
대한민국
560-250
전라북도전주시완산구중화산동한신코아아파트2동606호

한경은
대한민국
560-250
전라북도전주시완산구중화산동2가77-15번지

박혁규
대한민국
561-232
전라북도전주시덕진구인후2동1576-33번지

이민효
대한민국
442-726
경기도수원시팔달구영통동벽적골9단지주공아파트902-506

(74) 대리인 이건주

(77) 심사청구 없음

(54) 출원명 기가비트 이더넷 수동형 광 가입자망에서의 암호화 방법

요약

가. 발명이 속하는 기술분야

본 발명은 초고속 수동형 광 가입자망인 기가비트 이더넷 수동형 광 가입자망에 관한 것으로, 특히 기가비트 이더넷 수동형 광 가입자망의 암호화 방법에 관한 것이다.

나. 발명이 해결하고자 하는 기술적 과제

본 발명의 목적은 기가비트 이더넷 수동형 광 가입자망에서의 암호화 방법을 제공함에 있다.

다. 발명의 해결방법의 요지

본 발명은 하나의 광선로 종단장치와 적어도 하나의 광 가입자망 장치로 구성되는 기가비트 이더넷 수동형 광 가입자망에서, 발전된 암호화 표준 및 양방향 방식을 이용한 암호화 방법에 있어서, 광 가입자망 장치의 광선로 종단장치에 대한 등록과정과, 상기 등록과정에서 등록이 이루어진 광 가입자망 장치의 광선로 종단장치에 대한 인증과정과, 광선로 종단장치가 상기 인증과정에서 획득한 광 가입자망 장치의 공개키 값과 생성한 의사난수 값을 이용하여 세션키를 생성하는 과정과, 광선로 종단장치가 상기 의사난수 값을 광 가입자망 장치로 송신하는 과정과, 상기 의사난수 값을 수신한 광 가입자망 장치가 상기 인증과정에서 획득한 광선로 종단장치의 공개키 값과 상기 의사난수 값을 이용하여 세션키를 생성하는 과정을 포함함을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법을 제안한다.

라. 발명의 중요한 용도

기가비트 이더넷 수동형 광 가입자망의 보안유지를 위해 사용된다.

대표도

도8

색인어

기가비트 이더넷 수동형 광 가입자망(Gigabit Ethernet-Passive Optical Network, GE-PON), 암호화, 키, 스케줄링

명세서

도면의 간단한 설명

도 1은 수동형 광 가입자망의 구조를 도시하는 도면,

도 2는 AES 암호화 적용대상을 도시하는 도면,

도 3은 맥 제어 부계층을 중심으로 암호화키 정보가 포함된 정보교환 인터페이스를 도시하는 도면,

도 4는 암호화 구현을 위한 맥 제어 계층을 도시하는 도면,

도 5는 본 발명에 따른 도면으로, 광선로 종단장치 측면에서 이루어지는 암호화 단계들을 도시하는 도면,

도 6은 본 발명에 따른 도면으로, 광 가입자 장치에서 이루어지는 암호화 단계들을 도시하는 도면,

도 7은 본 발명에 따른 도면으로, 암호화를 위한 암호화키 생성 과정을 도시하는 도면,

도 8은 본 발명의 일 실시 예에.따른 도면으로, 암호화키 값 교환을 포함하는 광선로 종단장치와 광 가입자 장치와의 신호흐름을 도시하는 도면,

도 9는 본 발명의 다른 실시 예에 따른 광선로 종단장치와 광 가입자 장치와의 신호흐름을 도시하는 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 초고속 수동형 광 가입자망인 기가비트 이더넷 수동형 광 가입자망(Ethernet Passive Optical Network, EPON)에 관한 것으로, 특히 기가비트 이더넷 수동형 광 가입자망의 암호화 방법에 관한 것이다.

본 발명은 특히 기가비트 이더넷 수동형 광 가입자망에서의 암호화 방법 및 암호화 키 정보와 이에 따른 전체 스케쥴링 플로에 관한 것이다.

통상적으로, 정보를 뜻을 알 수 없는 정보(암호문)로 변환하는 것을 암호화라 한다. 암호화를 통해 정보를 암호문의 형태로 메모리에 저장하거나 통신 회선 상에서 전송함으로써 정보를 보호할 수 있다. 암호화를 세분하면, 통상적으로, 암호화와 복호화로 나누어 생각할 수 있다. 암호화는 암호화 키(특정한 비트 계열)를 사용하여 정보를 암호문으로 변환하는 것이고, 복호화는 복호 키를 써서 원래의 정보로 복원하는 것이다. 복호 키를 갖고 있는 사람만 올바른 정보로 복원할 수 있으므로, 복호 키가 제 3자에게 알려지지 않으면 정보를 보호할 수 있다. 암호 방식은 크게 비밀 키 암호 방식(관용 키 암호 방식)과 공개 키 암호 방식으로 나뉜다. 비밀 키 방식의 암호화와 복호화에 같은 키를 이용한다. 통신인 경우는 송신자와 수신자가 미리 똑같은 키를 비밀로 지닐 필요가 있다. 한편, 공개 키 암호 방식은 암호화와 복호화에 다른 키를 사용하며, 암호화 키는 공개하고 복호 키는 비밀로 한다. 실제로 이용되고 있는 것은 비밀 키 암호 방식이 많으며, 널리 알려진 방식으로는 DES(Data Encryption Standard)가 있다. 한편, 하기에서는 특별한 이유가 없는 한, '암호화'와 '복호화'를 구분하지 않고, 상기 '암호화'와 '복호화'를 통칭하여 "암호화"라 칭한다. 즉, 이하 사용되는 "암호화"라는 용어는 별도의 언급이 없는 한 상기 '암호화'와 '복호화'를 통칭하는 의미로 사용된다.

도 1은 수동형 광 가입자망 장치의 구성을 도시하고 있다.

도 1과 같이 수동형 광 가입자망은 하나의 광선로 종단장치(Optical Line Terminal, OLT, 이하 'OLT'라 칭함)(100)와 적어도 하나의 광 가입자망 장치(Optical Network Unit, ONU, 이하 'ONU'라 칭함)(120)들로 구성된다.

상기 도 1에 도시된 수동형 광 가입자망은 다시 비동기전송방식 수동형 광 가입자망과 기가비트 이더넷 수동형 광 가입자 망으로 구분할 수 있다. 한편, 현재에는 인터넷 기술의 발달과 가입자 측에서의 증가된 대역폭 요구에 따라 상대적으로 고가 장비이며 대역폭에 제한이 있고 IP 패킷을 세그먼테이션(segmentation)해야 하는 비동기전송방식 기술보다는 상대적으로 저가이며 높은 대역폭을 확보할 수 있는 기가비트 이더넷으로 종단간(end to end) 전송을 목표로 삼는 추세에 있다. 이에 따라 수동형 광 가입자 망 구조에서도 비동기전송방식이 아닌 이더넷 방식이 요구되고 있다.

비동기전송방식 수동형 광 가입자망(ATM-PON, APON)이 사용하고 있는 암호화 방안은 churning으로, 3바이트 크기의 암호화 키가 사용된다. 이 방법은 1초마다 암호화 키 값이 갱신되어야 하는 암호능력을 가지고 있으며 상대적으로 간단한 알고리즘이므로 622Mbps의 속도를 가지고 있는 APON에서 고속지원이 가능하기 때문에 APON에서 사용되었다. 이 방법에서 사용되는 암호화 키 값은 ONU(120)에서 만들어져 각 OLT(100)에게 제공되며 이 값과 주기적으로 갱신되는 암호화 키 값들은 유지보수(OAM) 셀의 페이로드(payload)부분에 넣어져 전달된다. APON의 경우, 당시 암호화기술의 한계와 고속지원의 가능성으로 인하여 3bytes의 churning 키를 유지보수 셀에 넣어 사용하였으나 이 경우, 암호화 키 자체의 능력이 제한된다는 문제점이 발생한다. 이에 비해, 기가비트 이더넷의 경우는 622Mbps의 전송속도를 갖는 APON에 비해 상대적으로 고속이므로 APON의 암호화방안을 따르는 것은 기술적으로 비효율적일 수밖에 없다. 또한 상대적으로 암호화에 취약한 점-대-다점의 구조를 가지고 있다. 따라서 이 경우, 상향/하향 링크의 사용자 데이터의 암호화문제가 중요하므로 강력하고 효율적인 암호화 키 방안의 선택과 효과적인 운용이 필요하다. 그러나 현재 기가비트 이더넷 수동형 광 가입자망의 암호화방안 및 암호화 키 관리 스케쥴링 방안은 IEEE802.3ah에서 표준화가 진행 중이다. 이에 따라 기가비트 이더넷 수동형 광 가입자망에 적합한 암호화 방법이 요구된다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 기가비트 이더넷 수동형 광 가입자망에서의 암호화 방법을 제공함에 있다.

본 발명의 다른 목적은 기가비트 이더넷 수동형 광 가입자망의 암호화에서 암호화키 관리 및 암호화키 값 교환에 따른 전체 스케쥴링 플로의 정의를 제공함에 있다.

상기 목적을 달성하기 위해 본 발명은; 하나의 광선로 종단장치와 적어도 하나의 광 가입자망 장치로 구성되는 기가비트 이더넷 수동형 광 가입자망에서, 발전된 암호화 표준 및 양방향 방식을 이용한 암호화 방법에 있어서, 광 가입자망 장치의 광선로 종단장치에 대한 등록과정과, 상기 등록과정에서 등록이 이루어진 광 가입자망 장치의 광선로 종단장치에 대한 인증과정과, 광선로 종단장치가 상기 인증과정에서 획득한 광 가입자망 장치의 공개키 값과 생성한 의사난수 값을 이용하여 세션키를 생성하는 과정과, 광선로 종단장치가 상기 의사난수 값을 광 가입자망 장치로 송신하는 과정과, 상기 의사난수 값을 수신한 광 가입자망 장치가 상기 인증과정에서 획득한 광선로 종단장치의 공개키 값과 상기 의사난수 값을 이용하여 세션키를 생성하는 과정을 포함함을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법을 제안한다.

발명의 구성 및 작용

이하 본 발명의 바람직한 일 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기에서 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다.

앞서 언급한 바와 같이, 이하 사용되는 "암호화"라는 용어는 별도의 언급이 없는 한 '암호화'와 '복호화'를 통칭하는 의미로 사용된다. 이에 따라 이하 사용되는 "암호화 키" 또한 '암호화 키'와 '복호 키'를 통칭하는 의미로 사용된다.

본 발명은 특히 기가비트 이더넷 수동형 광 가입자망에서의 암호화 방법 및 암호화 키 정보와 이에 따른 전체 스케쥴링 플로(flow)에 관한 것이다. 기가비트 이더넷 수동형 광 가입자망에서의 암호화를 고려할 시에 특히 중요시되어야 할 사항들은 사용자, 즉 ONU(120) 인증, 암호화(encryption), 그리고 암호화키 관리 등이다. 사용자 인증은 OLT(100)에서의 ONU(120) 등록기간 후에 실시되며 사용자 인증 전에는 각 ONU(120)들은 데이터를 주고받을 수 없다. 또한 상향 데이터와 하향 데이터를 암호화하는 것은 도청 방지와 비 인증 ONU(120)의 변장(impersonation)을 막기 위한 것이다. 이러한 사용자 인증과 암호화에는 암호화키가 사용되며 이 암호화키의 운용과 교환방식에 따라 암호화 방법의 암호화키 관리 플로와 스케쥴링이 달라진다.

한편, 본 발명에서 선택한, 기가비트 이더넷 수동형 광 가입자망에서 사용할 암호화 방법은 대칭적(symmetric)인 방법인 AES(Advanced Encryption Standard, 발전된 암호화 표준)으로 이는 Rijndael 알고리즘에 의해 구체화된다. AES는 DES보다 뛰어난 암호화 방법이며, 암호화키 갱신 주기가 3*1017 년이 되는 강력한 암호화 방법으로 특히 기가비트이상의 고속의 망을 위하여 제안되었다. AES 방법은 블록 단위로 데이터를 암호화하며, 이 때 블록의 크기는 128비트이다. AES 방법에서 사용되는 암호화키의 길이는 128, 192 혹은 256비트가 된다.

또, 본 발명에서는 암호화의 타입으로 공개키와 비밀키를 모두 사용하는 하이브리드(hybrid) 암호화방식을 선택하였다. 이는 공개키와 비밀키 방식의 장점만을 이용하기 위한 것으로, 분배키 값은 공개키를, 암호화방식은 대칭(symmetric)을 사용한다. 본 발명에서 OLT(100)와 ONU(120)는 상기 공개키와 비밀키의 두 키 값을 이용하여 세션키를 생성한다. 즉, OLT(100)와 ONU(120)가 상호 교환하는 공개키는 대칭적인 세션키를 생성하기 위한 목적으로 사용된다. 인증 프로토콜로는 X.509 표준의 양방향(two-way)방식을 선택하였는데, 이는 OLT(100)와 각 ONU(120)의 공개키 교환 시에 상호 인증서를 교환하기 위한 것이다. 본 발명에서는 인증서와 그 파라미터에 대한 별도의 언급을 생략한다.

도 2는 본 발명에서의 암호화 적용대상을 도시하는 도면이다.

본 발명에서는 특히 PDU(Packet Data Unit)(202)를 암호화 적용대상으로 한다. 도 2에서의 K(201)는 본 발명이 제안하는 암호화 방법에서 사용할 암호화키 값이 되며, 이하 이를 '세션키' 값이라 칭한다. 즉, 본 발명에서의 '세션키'는 본 발명이 제안하는 암호화 방법에서 사용하기 위해 생성하는 암호화키를 의미한다. 본 발명에서는 전술한 방식에서 ONU(120)와 OLT(100)가 교환하여야 할 암호화키 정보를 이더넷 맥 제어 프레임에 포함시켜서 하위 계층으로 전달한다. 상기 암호화키 정보를 이더넷 맥 제어 프레임에 포함시키는 과정은 맥 제어 계층(210)에서 이루어지며, 도 2의 AES 펑션(AES function)(204)에서 수행된다. AES 펑션(204)은 암호화 적용대상이 되는 PDU(202)에 상기 세션키 및 암호화를 위한 매개변수들에 포함시켜서 암호화가 이루어진 PDU(206)로 변환한다.

도 3은 암호화가 발생하는 기가비트 이더넷 수동형 광 가입자망 맥 제어 계

층을 중심으로 하여 상위의 맥 제어 클라이언트 부계층과 하위의 맥 계층 간에 교환되는 정보들을 나타내는 계층 간 서비스 인터페이스를 도시하는 도면으로, 도 3에서는 교환할 암호화키 값을 "KEY"으로 표시하였다. 도 3을 보면, 맥 제어 계층과 맥 계층사이에 주고받는 정보들이 목적지주소(DA), 소스주소(SA), 길이/타입(length/type), 데이터, 그리고 암호화키 값(KEY)이 되는 것을 볼 수 있다. 암호화의 각 단계에 따라 이 "KEY" 필드에 들어갈 내용들이 달라진다. 먼저 ONU(120)가 사용자 인증 요청 신호를 OLT(100)로 송신할 경우에는 ONU(120)의 공개키 값이, OLT(100)가 ONU(120)로 사용자 인증 응답 신호를 송신할 경우에는 OLT(100)의 공개키 값이, 세션키 생성단계에서는 의사난수 값(pseudo-random number)이 상기 "KEY" 필드에 들어간다.

도 4는 암호화 구현을 위한 맥 제어 계층을 도시하는 도면이다.

도 4는 ONU(120) 등록(REG, Registration), 레인징(ranging)(RNG, Ranging), 동적 대역 할당(Dynamic Bandwidth Allocation, DBA)등의 다른 맥 제어 기능(MAC control functionality)들과 함께 SDE(Secure Data Exchange)의 기능이 맥 제어 부계층(310)에 위치함을 도시하고 있다. 도 4의 상위계층(200)은 7계층 중 3계층 내지 7계층에 해당하며, 맥 클라이언트 부계층(300), 맥 제어 부계층(310), 맥 계층(220) 등은 2계층에 해당하고, 물리계층(410)은 1계층에 해당한다. 맥 클라이언트 부계층(300)은 LLC, bridge entity 등의 기능을 수행한다. 본 발명에서는 상기 2계층에서 기가비트 이더넷 수동형 광 가입자망의 암호화가 수행된다. 특히, 상기 맥 계층(220)과 REG, RNG, DBA, SDE 등의 기능을 수행하는 맥 제어 부계층(310)을 포함하는 계층을 기가비트 이더넷 수동형 광 가입자망 맥 계층(400)이라 한다.

도 5는 OLT 측면에서의 암호화 FSM(Finite State Machine)을 도시하고 있다.

도 5는 ONU(120)와 OLT(100)간의 다른 제어정보의 흐름과의 관계를 배제하고 암호화와 관련된 흐름만을 구성한 것으로, S0(500) 내지 S7(514)의 각 단계들은 다음과 같다. S0(500)은 초기화 단계, S1(502)은 인증단계, S2(504)는 공개키 획득단계, S3(506)은 세션키 생성단계, S4(508)는 세션키 공유단계, S5(510)는 활성화 단계, S6(512)은 새로운 세션키 생성단계, S7(514)은 키 교환 준비단계이다. 각각의 단계들에 대해 설명하면 다음과 같다.

먼저, S0(500) 상태에서 OLT(100)는 초기화를 수행한다. 초기화가 이루어지면 OLT(100)는 ONU(120)에서 보내온 인증요청(Authentication Request) 신호를 수신(503단계)하고 S1(502)의 인증상태로 진행한다. 상기 인증요청 신호에는 인증서가 포함되는데, X.509 프로토콜에 의하여 상기 인증서에는 송신한 ONU(120)의 공개키 값도 포함된다. 인증상태(502)에서 OLT(100)는 상기 ONU(120)의 신뢰도 등을 판단한다. 인증요청 신호를 통해 ONU(120)의 신뢰도가 인정되면 OLT(100)는 인증 응답신호를 상기 인증요청 신호를 송신한 ONU(120)로 송신한다(503단계). S2(504), 공개키 획득 단계에서 OLT(100)는 상기 ONU(120)의 공개키를 획득한다. 이로써 OLT(100)는 자신의 공개키, ONU(120)의 공개키, 그리고 자신의 비밀키를 알고 있는 상태가 된다. 상기 공개키는 상술한 바와 같이 인증요청 신호에 포함된다. 실제 데이터를 전송하기 위하여 OLT(100)는 ONU(120)의 공개키, 자신의 공개키, 자신의 비밀키의 세 가지 키 값과 의사난수 값을 이용하여 세션키를 생성한다. 세션키는 대칭적인 특징을 가지기 때문에 ONU(120)도 동일한 키 값을 가지고 있어야 하므로, 이 시점에서 OLT(100)는 ONU(120)에게 상기 의사난수 값을 전송한다. 이를 통해 OLT(100)와 ONU(120)는 세션키 값을 공유한다. OLT(100)는 ONU(120)로부터 세션키 생성완료 메시지를 수신한다(507). 이로서 세션키 생성이 완료되고, S4(508)의 세션키 공유 상태가 된다. 한편, 세션키 값이 생성된 이후에는 키 교환 시기 전까지 OLT(100)와 ONU(120)는 세션키 값과 AES 암호화방법을 이용하여 사용자 데이터를 암호화한다(S5 상태)(510). 상기 세션키를 생성하는 과정이 끝나면 기가비트 이더넷 수동형 광 가입자망의 암호화를 위한 기본적인 스케쥴링은 모두 끝난다. 이후의 시기는 일반적인 수동형 광 가입자망의 동작이 이어지고, 이는 새로운 세션키를 생성하기 전까지 계속된다.

한편, 암호화키 값 갱신(update) 시기에는 암호화키 값 갱신에 대해 몇 프레임 앞서부터 갱신시기를 알려 주기 위한 카운트다운 숫자가 들어간다. 이는 암호화키 동기 맞춤을 하기 위하여, 5 프레임 주기 이후에 암호화키 교환이 발생하는 경우 "5" 라는 숫자가, 4 프레임 주기 이후에 암호화키 교환이 일어나는 경우에는 "4"라는 식으로 교환이 발생할 때까지 삽입된다. 키 교환시기가 되면(S6상태)(512) OLT(100)는 현재까지의 세션을 종료하고 다시 의사난수 값을 ONU(120)로 송신함으로서 새로운 키를 생성한다. 한편, 도 5의 S1(502), S2(504), S3(506), S4(508), S5(510) 상태 각각에서 초기화 요구가 발생할 수 있으며, 초기화 요구가 발생할 시에는 S0(500) 상태로 천이한다.

도 6은 ONU 측면에서의 암호화 FSM을 도시한 것이다.

S0(600) 상태에서 초기화가 이루어지면 ONU(120)는 인증요청 신호를 OLT(100)로 송신한다(601단계). ONU(120)는 OLT(100)로부터 인증 응답 신호를 수신(603단계), 상기 인증 응답 신호에 포함된 OLT(100)의 공개키를 획득한다. ONU(120)는 상기 OLT(100)으로부터 의사난수 값을 수신(605단계)함으로써 세션키를 생성한다(S3)(606). 이에 따라 세션키 생성이 완료되고, OLT(100)와 ONU(120)는 세션키를 공유하는 상태가 된다. ONU(120)는 OLT(100)에게 세션키 생성완료 메시지를 송신한다(607단계). 세션키 값이 생성된 이후에는 OLT(100)와 ONU(120)는 키 교환 시기 전까지 상기 세션키 값과 AES 암호화방법을 이용하여 사용자 데이터를 암호화한다. 키 교환시기가 오면 ONU(120)는 현재까지의 세션을 종료하고 다시 OLT(100)로부터 의사난수 값을 수신함으로서 새로운 키를 생성한다.

도 7은 도 5와 도 6의 단계들을 타이밍도로 표현한 것이다.

도 7은 OLT(100) 및 ONU(120)가 서로의 공개키와 자신의 비밀키를 알고 있는 상태에서 세션키를 생성하고 데이터를 전송하는 흐름을 나타낸다. 도 7에 도시된 바와 같이, 세션키 K는 f(a, aP, bP, r)의 입력 파라미터를 가지고 있는 함수로 생성되며(704), 제 701단계에서 OLT(100)는 ONU(120)와 동일한 세션키를 생성하기 위하여 의사난수 값 r을 ONU(120)로 전송한다. 상기 의사난수 값을 수신한 ONU(120)는 세션키를 생성하고(706) 703단계에서 세션키 생성 완료 메시지를 OLT(100)로 송신한다. 제 705단계에서 OLT(100) 데이터를 전송할 슬롯의 위치, 크기 등의 정보를 포함하는 통상의 그랜트 신호를 ONU(120)로 송신한다. 상기 통상의 그랜트(normal grant) 신호는 ONU(120)들의 인증요구가 충돌하지 않게 하기 위하여 각각의 ONU(120)가 인증요구를 할 수 있는 슬롯 위치(slot position)와 슬롯 크기(slot size) 등을 명시한 신호이다. 이 때의 그랜트 신호의 종류를 인증 그랜트로 하여 통상의 그랜트 신호의 그랜트 형태 필드(grant type field)에 설정한다. 제 707단계에서 ONU(120)는 수신한 통상의 그랜트 신호에 포함된 정보에 따라 OLT(100)로 데이터를 송신한다.

도 8은 본 발명의 일 실시 예에 따른 도면으로, 암호화 절차를 GE-PON의 일반적인 스케쥴링 절차와 함께 도시한 도면이다.

도 8의 제 801단계 내지 제 805단계가 ONU 등록 단계에 해당한다. 제 801단계에서 OLT(100)는 ONU(120)들에게 등록 그랜트(Registration Grant) 신호를 송신함으로서 각 ONU(120)들의 등록요청 신호 송신을 허가한다. 제 803단계에서 ONU(120)들은 상기 등록 그랜트의 정보에 따라 자신에게 할당된 시간에 등록 요청 신호를 송신하여 ONU(120) 등록을 한다. 제 805단계에서 OLT(100)는 등록된 ONU(120)들에게 인증 그랜트 신호를 송신한다. 제 807단계 내지 제 811단계는 인증 및 공개키 획득 단계이다. 제 807단계에서 OLT(100)는 등록이 이루어진 ONU(120)들에 대해 인증 그랜트 신호를 송신한다. 상기 인증 그랜트 신호를 수신한, 등록된 ONU(120)들은 제 809단계에서 OLT(100)에게 인증 요청 신호를 송신한다. 제 811단계에서 OLT(100)는 상기 ONU(120)들 중 인증이 이루어진 ONU(120)들에게 인증 응답 신호를 송신한다. 상기 인증 요청 신호 및 인증 응답 신호를 통해 OLT(100)와 ONU(120)들은 각각 상대의 공개 키 값을 획득하게 된다. 제 813단계 내지 제 815단계는 세션키 생성 단계이다. 제 813단계에서 OLT(100)는 세션키 생성에 이용한 의사난수 값을 ONU(120)로 송신한다. 상기 의사난수 값을 수신하여 세션키를 생성한 ONU(120)는 제 815단계에서 세션키 생성 완료 메시지를 OLT(120)로 송신한다. 이로써 암호화와 관련된 절차가 완료되며, 새로운 세션키 생성 요구가 발생할 때가지 상기 생성된 세션키를 이용하여 데이터 전송이 이루어진다. 제 817단계 이하의 단계들은 통상적인 통신 단계에 해당하므로 이에 대한 설명은 생략한다.

상기 도 8에 도시된 실시 예에서는 ONU(120)가 OLT(100)에 등록을 하고 상기 OLT(100)로부터 ONU(120) ID를 부여받은 후에 사용자 인증을 하는 과정을 도시한다. 상기 실시 예에서는 등록 시에 발생하는 충돌로 인한 손실에는 영향을 받지 않는다는 장점이 있다.

또, 도 9에 도시된 바와 같이, 사용자 인증을 한 후, 인증 받은 ONU(120)만 OLT(100)에 등록을 하는 방법을 고려하면 도8 의 실시 예에서 사용자의 신뢰성을 확인하지 않은 채로 아이디를 부여하는 점과 도8 의 전체 스케쥴링 절차를 줄일 수 있다.

이 방법은 신뢰성이 확인된 사용자만이 등록을 할 수 있다. 즉, 충돌을 경험하지 않고 성공적으로 등록 요청을 한 ONU(120)라고 하여도 인증할 수 없는 경우에는 ONU(120) ID를 부여하지 않는다. 이는 전체적인 스케쥴링 절차가 감소한다는 장점이 있다. 도 9에 도시된 과정들을 설명하면 다음과 같다. 제 901단계에서 OLT(100)는 ONU(120)로 등록 그랜트 신호를 송신한다. 제 903단계에서 ONU(120)는 등록 요청 신호 및 인증 요청 신호를 함께 OLT(100)로 송신한다. OLT(100)에서 ONU(120)의 등록과정이 끝나면 상기 OLT(100)는 등록된 ONU(120)에게 인증을 요구할 수 있는 인증 그랜트(grant) 신호를 송신한다. 제 905단계에서 OLT(100)는 등록 응답 신호 및 인증 응답 신호를 상기 ONU(120)로 송신한다. 이와 같이 등록과 인증이 한번에 이루어지므로, OLT(100)는 별도의 인증 그랜트 신호를 ONU(120)로 송신할 필요가 없다. 제 907단계에서 OLT(100)는 세션키 생성에 이용한 의사난수 값을 ONU(120)로 송신한다. 상기 의사난수 값을 수신하여 세션키를 생성한 ONU(120)는 제 909단계에서 OLT(100)로 세션키 생성 완료 메시지를 송신한다. 제 911단계 이하의 단계들은 통상적인 통신 단계에 해당하므로 이에 대한 설명은 생략한다.

발명의 효과

본 발명은 기가비트 이더넷 수동형 광 가입자망에서의 적절한 암호화방법을 선택하고, 이를 운용하기 위한 암호화키 값의 교환과 운용방법을 수동형 광 가입자망의 스케쥴링 절차에 포함시켜 정의한 것으로, 보안에 취약한 점-대-다점 구조를 가지는 기가비트 이더넷 수동형 광 가입자망에서의 효율적인 암호화 절차를 수행할 수 있다.

(57) 청구의 범위

청구항 1.

하나의 광선로 종단장치와 적어도 하나의 광 가입자망 장치로 구성되는 기가비트 이더넷 수동형 광 가입자망에서, 발전된 암호화 표준 및 양방향 방식을 이용한 암호화 방법에 있어서,

광 가입자망 장치의 광선로 종단장치에 대한 등록과정과,

상기 등록과정에서 등록이 이루어진 광 가입자망 장치의 광선로 종단장치에 대한 인증과정과,

광선로 종단장치가 상기 인증과정에서 획득한 광 가입자망 장치의 공개키 값과 생성한 의사난수 값을 이용하여 세션키를 생성하는 과정과,

광선로 종단장치가 상기 의사난수 값을 광 가입자망 장치로 송신하는 과정과,

상기 의사난수 값을 수신한 광 가입자망 장치가 상기 인증과정에서 획득한 광선로 종단장치의 공개키 값과 상기 의사난수 값을 이용하여 세션키를 생성하는 과정을 포함함을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 2.

제 1항에 있어서,

세션키를 생성한 광 가입자망 장치가 세션키 생성 완료 메시지를 광선로 종단장치로 송신하는 과정을 더 포함함을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 3.

제 1항에 있어서,

상기 인증과정은 광선로 종단장치로부터 인증 그랜트 신호를 수신한 광 가입자망 장치가 상기 광선로 종단장치로 인증 요청 신호를 송신하는 과정과,

상기 광선로 종단장치로부터 인증 응답 신호를 송신하는 과정으로 이루어짐을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 4.

제 3항에 있어서,

상기 인증 요청 신호•및 인증•응답 신호는 각각 광 가입자망 장치와 광선로 종단장치의 공개키 값을 포함함을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 5.
제 1항에 있어서,

상기 광선로 종단장치가 생성하는 세션키는 광선로 종단장치의 공개 키 및 비밀 키 값과, 광 가입자망 장치의 공개 키 값과, 광선로 종단장치가 생성한 의사난수 값 등을 이용하여 생성됨을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 6.
제 1항에 있어서,

상기 광 가입자망 장치가 생성하는 세션키는 광 가입자망 장치의 공개 키 및 비밀 키 값과, 광선로 종단장치의 공개 키 값과, 광선로 종단장치로부터 수신한 의사난수 값 등을 이용하여 생성됨을 특징으로 하는 기가비트 이더넷 광 가입자망의 암호화 방법.

청구항 7.
하나의 광선로 종단장치와 적어도 하나의 광 가입자망 장치로 구성되는 기가비트 이더넷 수동형 광 가입자망에서, 발전된 암호화 표준 및 양방향 방식을 이용한 암호화 방법에 있어서,

광 가입자망 장치가 광선로 종단장치로부터 등록 그랜트 신호를 수신하는 과정과,

광선로 종단장치로 등록 요청 신호를 송신하는 과정과,

상기 광선로 종단장치로부터 인증 그랜트 신호를 수신하는 과정과,

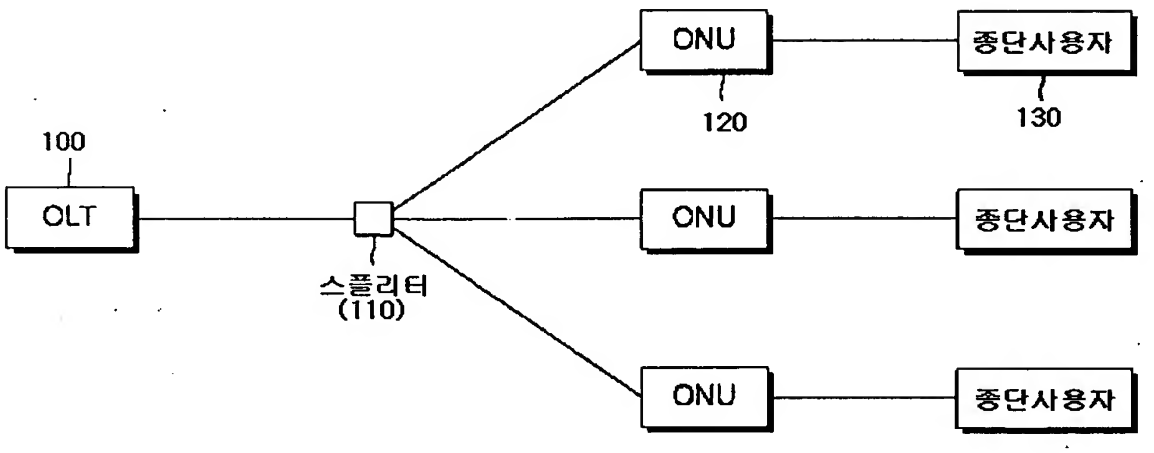
상기 인증 그랜트 신호에 따라 상기 광선로 종단장치로 인증 요청 신호를 송신하고, 상기 광선로 종단장치로부터 인증 응답 신호를 수신하는 과정과,

상기 광선로 종단장치로부터 의사난수 값을 수신하는 과정과, 상기 의사난수 값과 상기 인증 응답 신호에 포함된 상기 광선로 종단장치의 공개키 값을 이용하여 세션키를 생성하는 과정과,

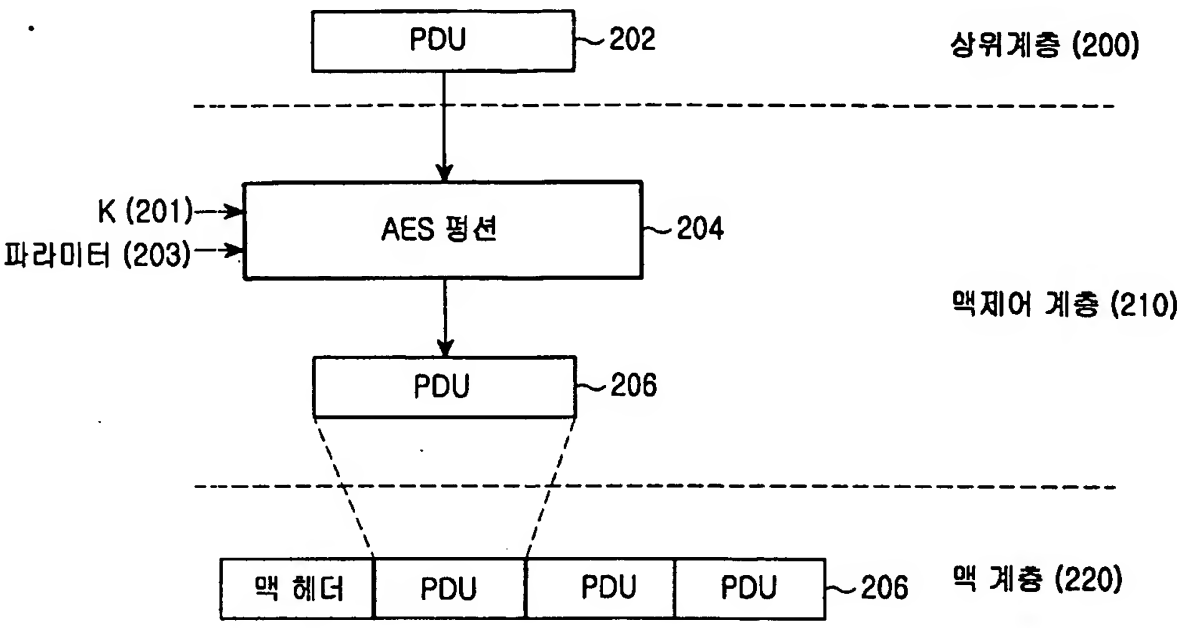
사용자 데이터를 상기 세션키를 이용한 발전된 암호화 방식으로 암호화하여 송신하는 과정으로 이루어짐을 특징으로 하는 기가비트 이더넷 광 가입자망 장치의 암호화 방법.

도면

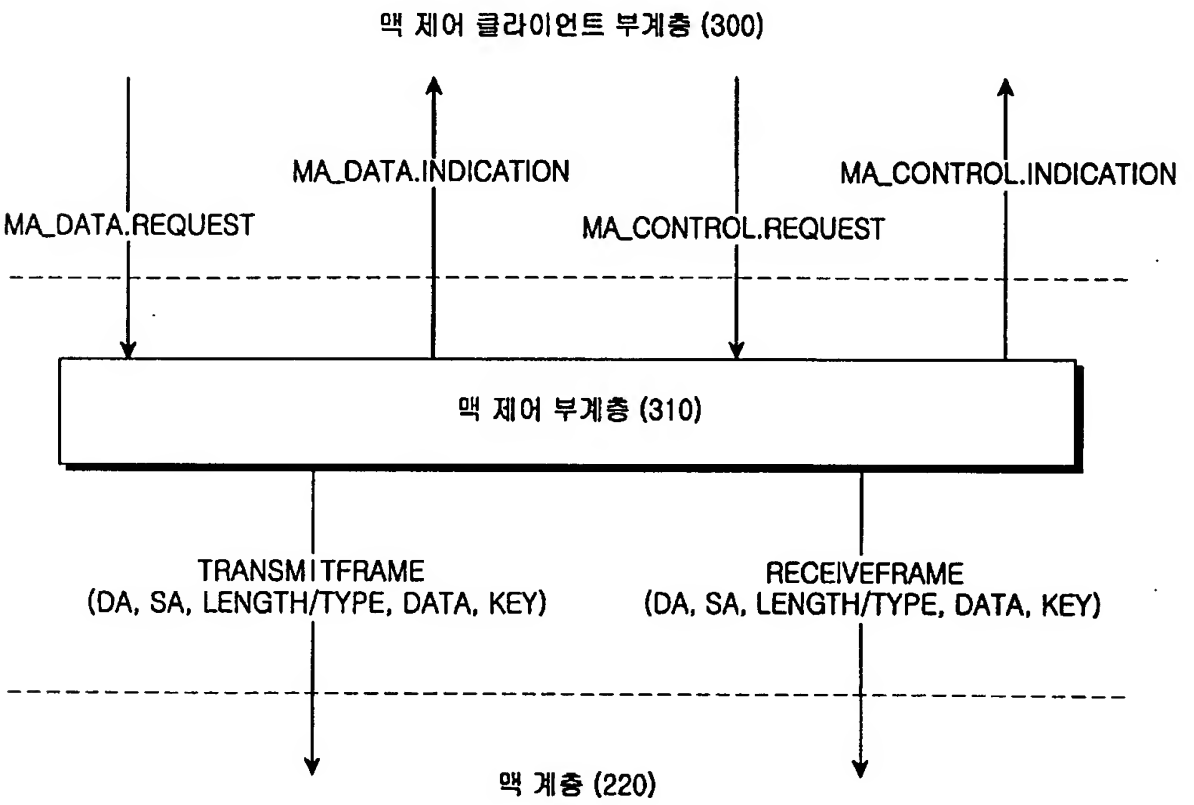
도면 1



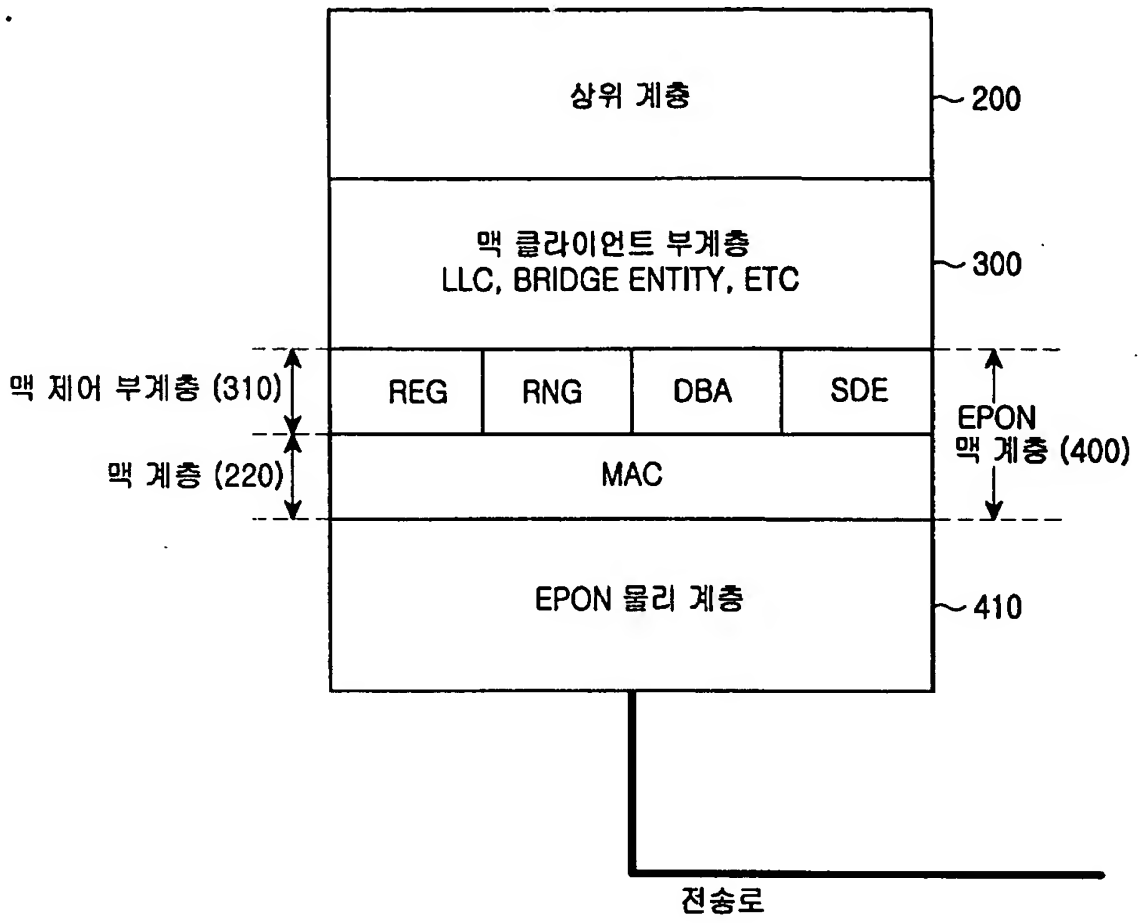
도면 2


PDU
202
상위계층 (200)
K (201)
파라미터 (203)
AES 펑션
204
맥제어 계층 (210)
PDU
206
맥 헤더
PDU
PDU
PDU
206
맥 계층 (220)

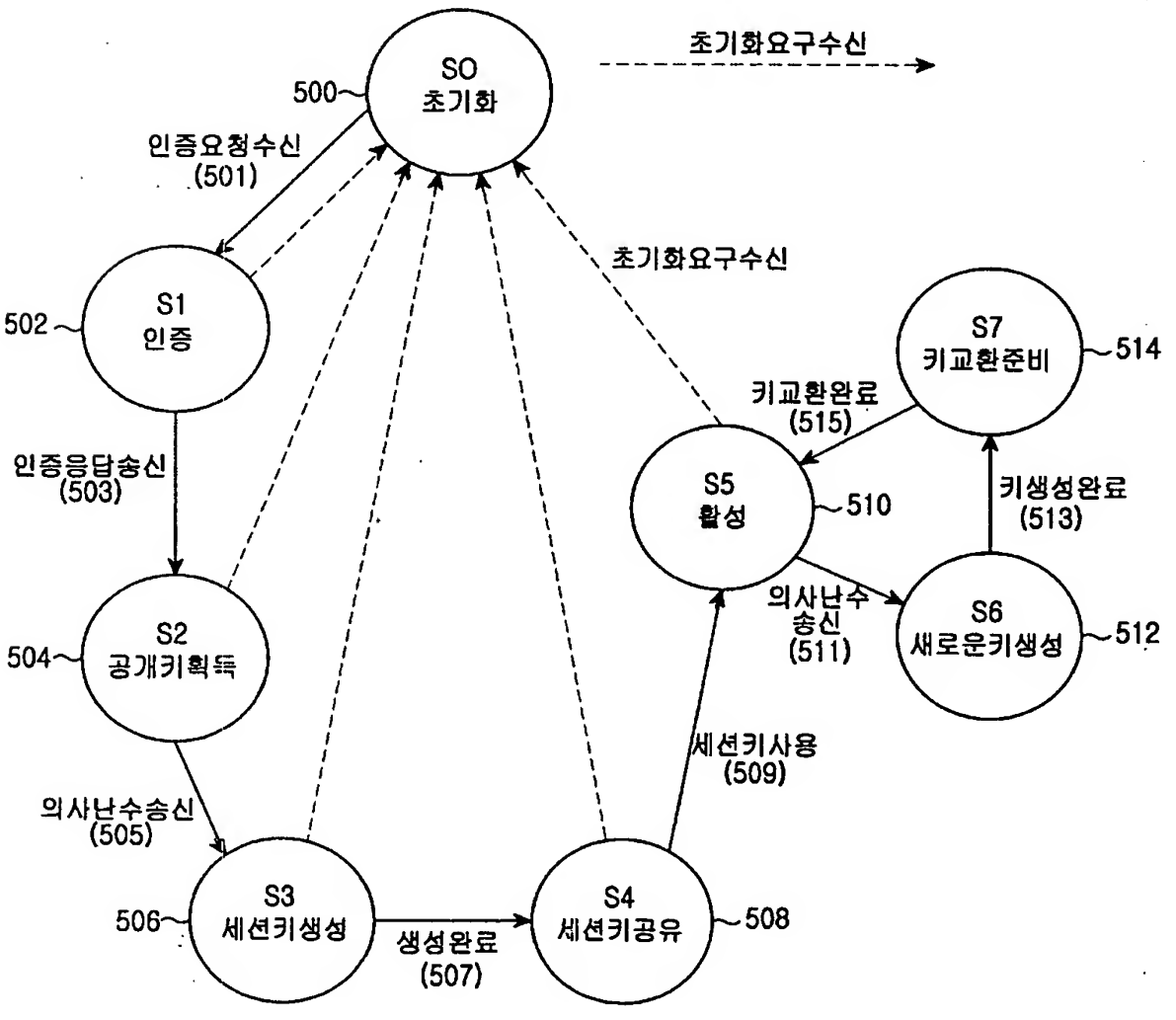
도면 3


맥 제어 클라이언트 부계층 (300)
MA_DATA.REQUEST
MA_DATA.INDICATION
MA_CONTROL.REQUEST
MA_CONTROL.INDICATION
맥 제어 부계층 (310)
TRANSMITFRAME
(DA, SA, LENGTH/TYPE, DATA, KEY)
RECEIVEFRAME
(DA, SA, LENGTH/TYPE, DATA, KEY)
맥 계층 (220)

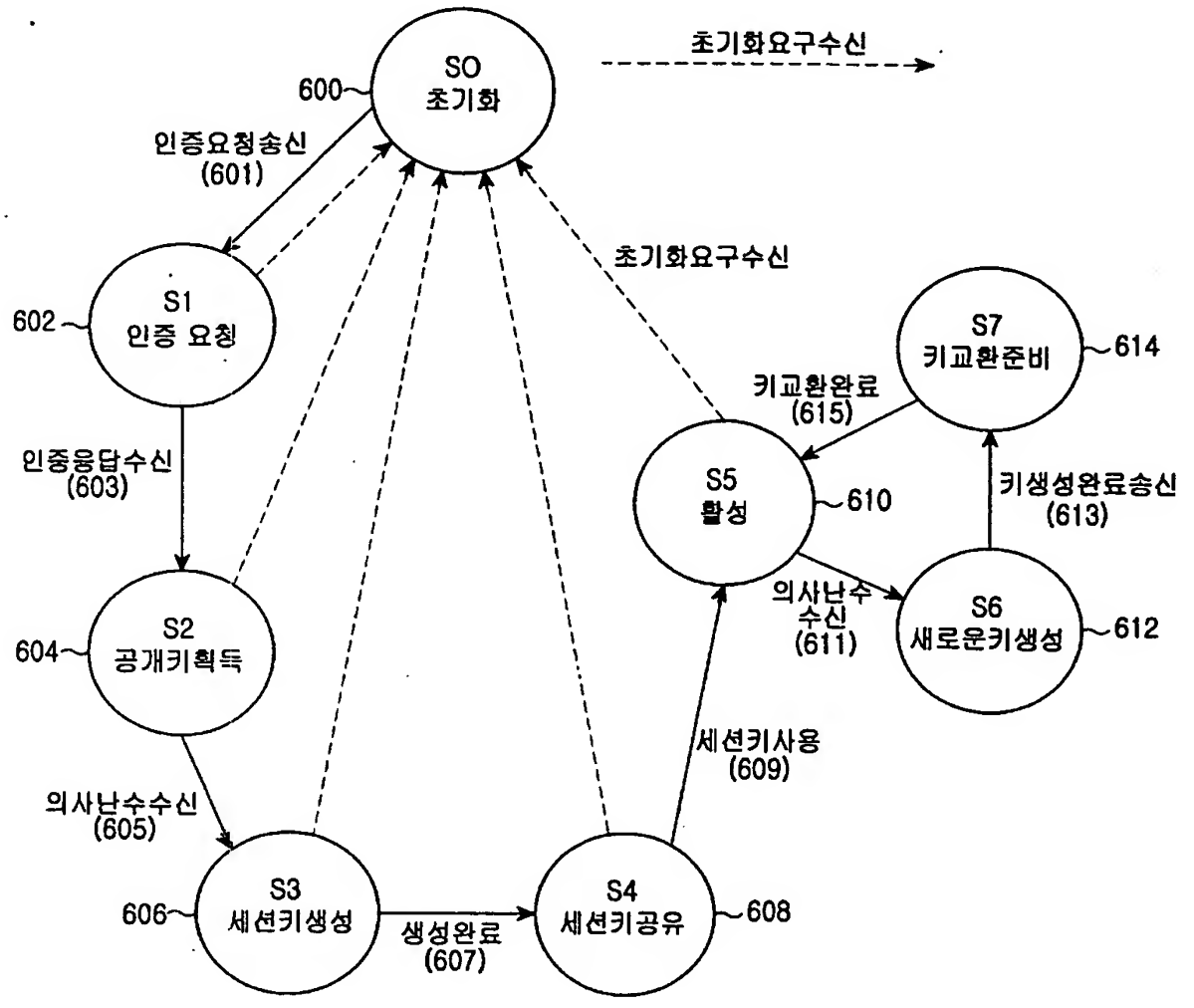
도면 4


상위 계층
200
맥 클라이언트 부계층
LLC, BRIDGE ENTITY, ETC
300
맥 제어 부계층 (310)
REG
RNG
DBA
SDE
EPON
맥 계층 (400)
맥 계층 (220)
MAC
EPON 물리 계층
410
전송로

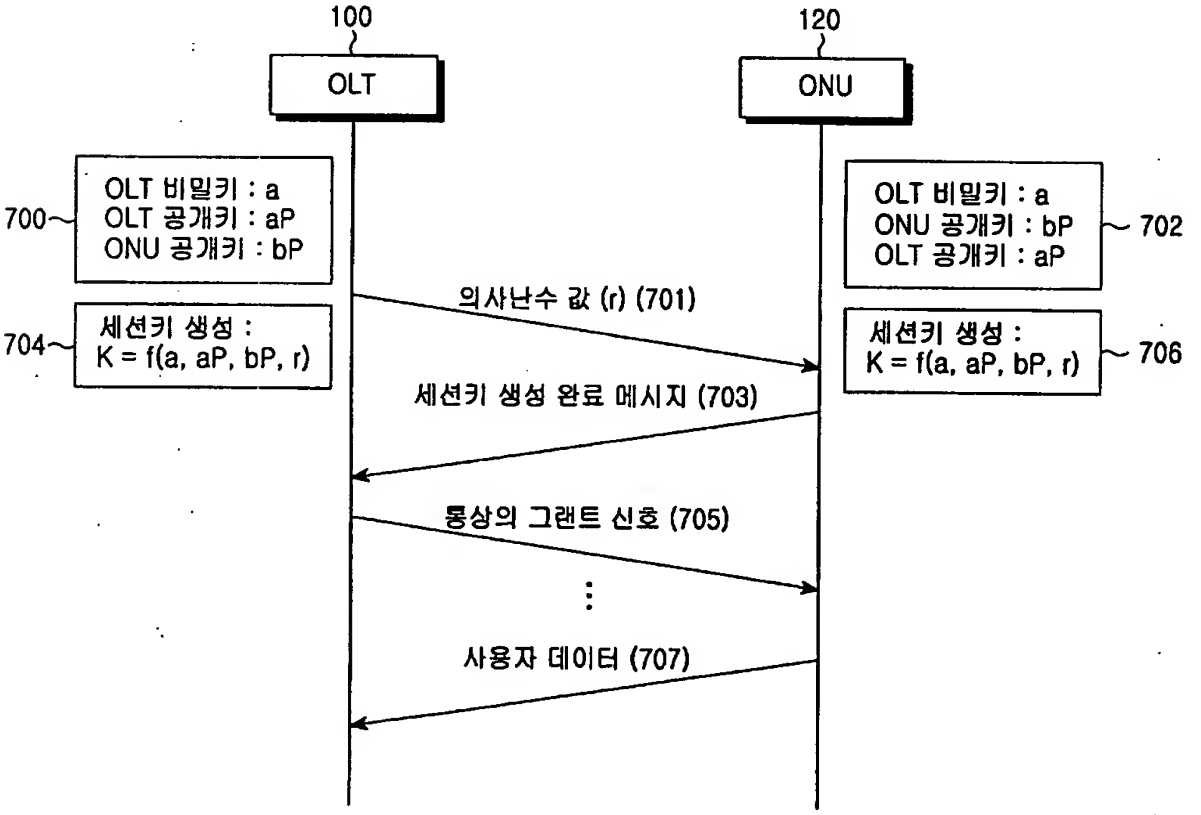
도면 5


SO
초기화
500
초기화요구수신
인증요청수신
(501)
초기화요구수신
S1
인증
502
S7
키교환준비
514
키교환완료
(515)
인증응답송신
(503)
S5
활성
510
키생성완료
(513)
의사난수
송신
(511)
S6
새로운키생성
512
S2
공개키획득
504
세션키사용
(509)
의사난수송신
(505)
S3
세션키생성
506
생성완료
(507)
S4
세션키공유
508

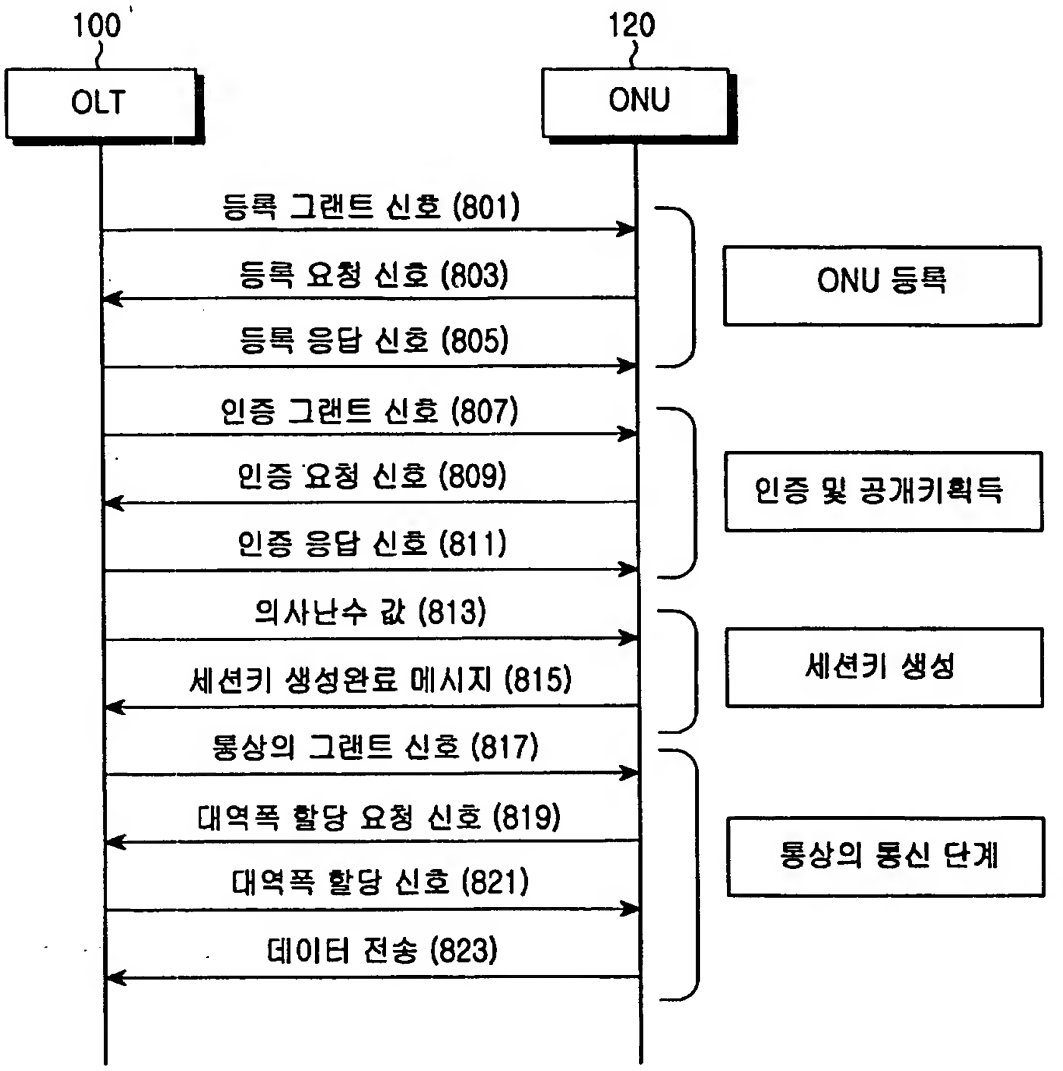
도면 6


SO
초기화
600
초기화요구수신
인증요청송신
(601)
초기화요구수신
S1
인증 요청
602
인증응답수신
(603)
S2
공개키획득
604
의사난수수신
(605)
S3
세션키생성
606
생성완료
(607)
S4
세션키공유
608
세션키사용
(609)
S5
활성
610
의사난수
수신
(611)
S6
새로운키생성
612
키생성완료송신
(613)
키교환완료
(615)
S7
키교환준비
614

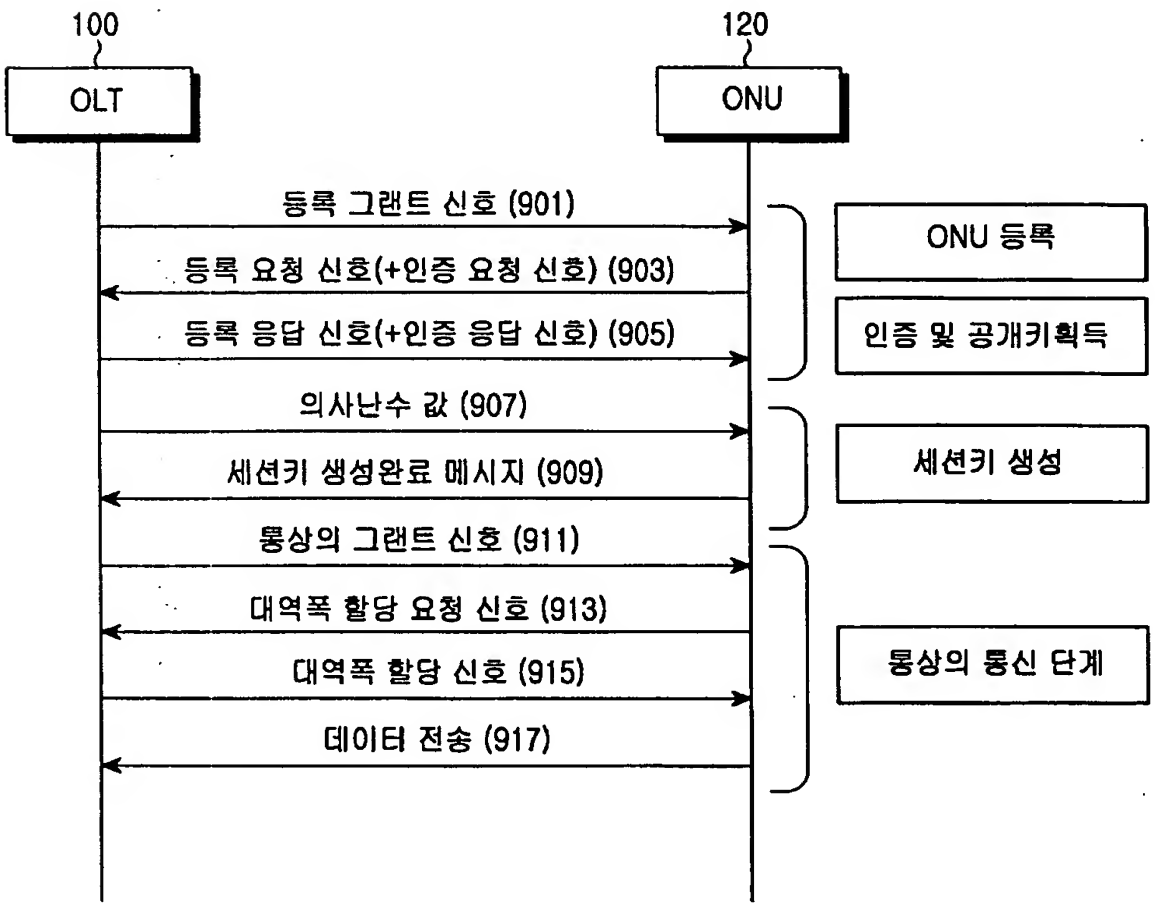
도면 7


100
OLT
120
ONU
OLT 비밀키 : a
OLT 공개키 : aP
ONU 공개키 : bP
700
OLT 비밀키 : a
ONU 공개키 : bP
OLT 공개키 : aP
702
의사난수 값 (r) (701)
세션키 생성 :
K = f(a, aP, bP, r)
704
세션키 생성 :
K = f(a, aP, bP, r)
706
세션키 생성 완료 메시지 (703)
통상의 그랜트 신호 (705)
사용자 데이터 (707)

도면 8


100
120
OLT
ONU
등록 그랜트 신호 (801)
등록 요청 신호 (803)
등록 응답 신호 (805)
ONU 등록
인증 그랜트 신호 (807)
인증 요청 신호 (809)
인증 응답 신호 (811)
인증 및 공개키획득
의사난수 값 (813)
세션키 생성완료 메시지 (815)
세션키 생성
통상의 그랜트 신호 (817)
대역폭 할당 요청 신호 (819)
대역폭 할당 신호 (821)
데이터 전송 (823)
통상의 통신 단계

도면 9


100
120
OLT
ONU
등록 그랜트 신호 (901)
등록 요청 신호(+인증 요청 신호) (903)
등록 응답 신호(+인증 응답 신호) (905)
ONU 등록
인증 및 공개키획득
의사난수 값 (907)
세션키 생성완료 메시지 (909)
세션키 생성
통상의 그랜트 신호 (911)
대역폭 할당 요청 신호 (913)
대역폭 할당 신호 (915)
데이터 전송 (917)
통상의 통신 단계